

Electronic Signature and Its Evidentiary Value in Electronic Commerce Transactions

BENNOUI Khaled, Mohamed El Bachir El Ibrahimi University, Bordj Bou Arreridj, Algeria, khaled.bennoui@univ-bba.dz

Send Article Date: 2026-03-19

Date of acceptance of the article 07-05-2026 :

Abstract: The technical Guaranties to Accredite The Electronic Signature as a means to prove the Electronic Trade Dealings

The electronic trade had resulted new concepts adapted to the specificities featured their dealings, and among these concepts the electronic signature which is considered as a tool or a mean of evidences of them, and due to what the electronic dealings imposed of special problems in the aspect of confidence.so ; it is obligatory upon the dealers in its field to find guaranties enhancing this type of dealings.

Key words : The Electronic signature, the encoding, the electronic accreditation, testifying of the electronic accreditation,

Introduction

If proof is of utmost importance in traditional legal dispositions and contracts, stemming from the premise that "everyone who claims a right must provide evidence of its existence, because proof is the strength of the right, and any right without proof is tantamount to non-existence", then this importance is of a higher degree in electronic commerce contracts. These are considered contracts of a special nature, characterized by their "paperless" quality on the one hand, and on the other, because they are concluded remotely via modern electronic means that have altered the concepts previously existing in the field of proof.⁽¹⁾

This distinctiveness has led to the emergence of new terminologies compatible with the modern technologies employed in this type of contract. Electronic records appeared, followed by electronic writing as a substitute for paper records and handwritten script, just as the electronic signature emerged as a substitute for the handwritten or traditional signature.

While it is established that the signature is the fundamental element in a legally valid written proof -since it is the sole means capable of attributing the document to its

¹. Anwar Sultan: Rules of Evidence in Civil and Commercial Matters, A Study in Egyptian and Lebanese Law, 1st Ed., Lebanon, Beirut, Dar Al-Jamiiyya for Printing and Publishing, 1984, p. 5.

issuer - the use of modern communication means in transactions has rendered the concept of the traditional signature incompatible with electronic documents. These documents possess a specific nature distinct from paper documents, a matter which led to the emergence of a new type of signature: the "electronic signature".

While this type of signature poses a challenge regarding its concept, it poses an even greater challenge regarding the guarantees for its adoption, especially since it is executed on an electronic medium remotely, and particularly since it frequently concerns material matters.

Consequently, this research paper will discuss these issues by elucidating its concept (First), and then addressing the guarantees of confidence therein (Second).

First: The Concept of the Electronic Signature

The concept of the electronic signature can be determined by addressing its definition and then outlining its forms, in detail as follows:

1- Definition of the Electronic Signature

A signature is generally defined as: "A personal mark or inscription placed by the signatory to confirm the correctness of the document's content and the veracity of what is written therein, along with their acknowledgment of responsibility for what it contains". Thus, the signature is a written mark or a sign placed by the signatory on the document, binding them to its content. The signature is not required to be in a specific form; the important thing is that it indicates its owner. This indication is realized through leaving a distinct, visible trace that remains and does not vanish immediately after completion, as this is the evidence of the signatory's intention to commit to the content of the document.⁽¹⁾

Proof by writing requires that the document presented as evidence be signed by the person to whom it is attributed. This applies whether the document is official or customary. Furthermore, various laws and legislations consider the signature as a right inherent to the personality, meaning that the person must place their signature on the document attributed to them personally, i.e., by their own hand action (whether the signature is done directly by hand, i.e., a manuscript signature, or by a fingerprint, or by a personal seal), with the exception of certain cases where they may delegate their signature to another person, such as a person permitting another to use their private seal and place it on a specific document. In this case, it is stipulated that the seal be placed with the approval of its owner and in their presence ⁽²⁾

Accordingly, we can deduce that the signature is, on one hand, a means not subject to doubt for determining the identity of the signatory, and on the other hand, a clear expression of the signatory's intention to commit to the content of the signed document

¹. Paule Robert: Le Nouveau petit Robert de la langue Française, texte remonté et amplifié sous la direction de: Josette Reuy-Delove et Alain Rey, Paris, édition Sejer, 2008, Maury p. 2371.

². See: Najwa Abu Heiba: The Electronic Signature: Definition and Evidentiary Validity, Cairo, Dar Al-Nahda Al-Arabiya, n.d., p. 39.

and their approval thereof; and thirdly, it is evidence of the presence of the parties to the disposition at the time of signing⁽¹⁾

This applies to the traditional signature. As for the electronic signature, which emerged as a necessity of electronic commerce and the revolution of information and communication technology, it has been addressed by various studies which presented different definitions, whether at the level of jurisprudence, organizations, or various legislatures. We will attempt to address the most important definitions provided, as space does not allow for mentioning all definitions, as follows:

The electronic signature was first addressed in the UNCITRAL Model Law on Electronic Commerce of 1996. Article 7 of this Law stipulated that: "Where the law requires a signature of a person, that requirement is met in relation to a data message if: (a) A method is used to identify that person and to indicate that person's approval of the information contained in the data message; and (b) That method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement"⁽²⁾

It is clear from this text that the Model Law required the electronic signature to perform the functions of the traditional signature, namely: distinguishing the identity of the signatory, and expressing their consent regarding the conclusion of the legal act contained in the signed document, without stipulating a specific method or procedures for such a signature. The important thing is that it is done through a reliable method. Thus, it has left every state absolute freedom to determine the methods and procedures of the electronic signature in accordance with its own legislation⁽³⁾

The European Directives also defined it pursuant to Directive No. 1999/93/EC dated December 13, 1999, concerning a common framework for electronic signatures⁽⁴⁾ as: "Data in electronic form attached to or logically associated with other electronic data and used as a means of proving their validity"⁽⁵⁾.

In 2001, the UNCITRAL Model Law on Electronic Signatures was issued by the United Nations Commission on International Trade Law⁽⁶⁾. This Law defined the electronic signature in Paragraph (a) of Article 2, which stipulated: "(a) 'Electronic signature' means data in electronic form in, affixed to or logically associated with, a data

¹. Mohamed El-Morsi Zahra: Civil Protection for Electronic Commerce, 3rd Ed., Cairo, Dar Al-Nahda Al-Arabiya, n.d., p. 225.

². UNCITRAL Model Law on Electronic Commerce.

³. See: Iman Mamoun Ahmed Suleiman: Conclusion and Proof of the Electronic Contract: Legal Aspects of the Electronic Commerce Contract, 1st Ed., Alexandria, Dar Al-Jami'a Al-Jadida, 2008, p. 249.

⁴. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, JOCE, 19 January 2000.

⁵. The electronic signature is defined as "data in electronic form, which is attached to or logically associated with other electronic data and which serves as a method of identification", JOCE, 19 January 2000, L. 13, p12.

⁶. The Model Law on Electronic Signatures issued on December 12, 2001, adopted by the United Nations General Assembly in its 56th session held on January 24, 2002, under item 161 of the agenda, Resolution No. 56/80.

message which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message"⁽¹⁾

At the level of legislations, many legislators attempted to define this type of signature, as it is one of the novelties imposed by electronic commerce on the one hand, and on the other hand, because it is the tool capable of achieving confidence and security in electronic transactions in general, regardless of their field, thus encouraging their adoption due to the advantages they provide. Among the legislations that defined the electronic signature, we mention, by way of example and not limitation:

1- French Legislation: Initially, the French Civil Code was devoid of any definition of the signature, like most civil codes worldwide, as the task of defining terminology is usually entrusted to jurisprudence. However, this was rectified through Law No. 2000-230 of March 13, 2000, regarding the adaptation of the rules of evidence to information technologies relating to the electronic signature. This law added new texts to the Civil Code containing a set of amendments consistent with the developments in the field of communication technologies and their repercussions on transactions. It defined the signature pursuant to the text of Article 1316-4/1, which stated: "The signature required for the perfection of a legal act identifies the person who appends it. It manifests the consent of the parties to the obligations arising from that act. When it is appended by a public officer, it authenticates the act"⁽²⁾

It is noted regarding this definition that it is a general definition encompassing all forms of signatures: manuscript, fingerprint, seal, electronic signatures, and others. It is also an abstract definition because it focused on the function of the signature regardless of its method; the important thing is that it identifies the signatory on the one hand, and expresses their will to accept the content of the document they signed and to commit to it on the other hand. If the signature is issued by a competent public officer, it confers the official character upon the document bearing it⁽³⁾. Then, the French legislator affirmed the electronic signature in the second paragraph of the same Article, which stated: "When the signature is electronic, it consists of the use of a reliable process of identification which guarantees its link with the act to which it relates. The reliability of this process is presumed, until proof to the contrary, when the electronic signature is created, the identity of the signatory ensured, and the integrity of the act guaranteed, pursuant to conditions fixed by decree in the Council of State"⁽⁴⁾.

¹. The Model Law on Electronic Signatures issued on December 12, 2001, adopted by the United Nations General Assembly in its 56th session held on January 24, 2002, under item 161 of the agenda, Resolution No. 56/80.

². Article 1316-4/1 of the Civil Code: "La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte". J.O du 14 mars 2000, P3968.

³. See: Ali Sayed Qassem: "Some Legal Aspects of the Electronic Signature", Journal of Law and Economics for Legal and Economic Research, No. 72, 2002, p. 40.

⁴. Article 1316-4, paragraph 2, reserved for the electronic signature, states that: "lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en conseil d'Etat."

Through this text, the legislator clarified that the electronic signature, which is carried out via a secure means, is considered a legal presumption that it is a reliable signature until proven otherwise. However, he did not specify the means capable of achieving security for the electronic signature or the conditions of such security, but rather left the matter to the Council of State.

2- Algerian Legislation: The Algerian legislator was interested in the electronic signature as an imperative necessity for electronic transactions, from which the Algerian citizen was not isolated despite the absence of special legislation. The beginning of interest was through Law No. 05-10 previously referred to. This law included the amendment of some articles of the Civil Code and the addition of others, in line with the repercussions of the information and communication technology revolution on the transaction aspect. The legislator referred to the electronic signature in the amended Article 327, where its second paragraph stipulated: "The electronic signature is recognized according to the conditions mentioned in Article 323 bis 1 above"⁽¹⁾. This implies that this amendment sufficed by indicating the necessity for the electronic signature to achieve the possibility of verifying the identity of its issuer, and that it be prepared and preserved under conditions guaranteeing its integrity, without reference to the concept or form of the electronic signature.

This matter led those interested in this field to consider that the amendments made by the legislator at the level of the Civil Code are insufficient to encompass all aspects of the electronic signature and its implications, and that it is necessary to issue a special law for the electronic signature.

This indeed occurred after a long wait, as the Algerian legislator issued Law No. 15-04 dated 11 Rabi' al-Thani 1436 AH corresponding to February 1, 2015 AD, defining the general rules related to electronic signature and electronic certification⁽²⁾. The Algerian legislator defined the electronic signature pursuant to Article 2/1 of this Law, which stipulated: "1- Electronic signature: Data in electronic form attached to or logically associated with other electronic data used as a means of authentication"⁽³⁾. This definition did not deviate from what was stated in the European Directives and French Law.

After presenting these definitions provided for the electronic signature, we can say that whether at the level of organizations, legislations, or even jurisprudence, care was taken to clarify what the signature must achieve, namely: determining the identity of the signatory and distinguishing them from other persons, and the diversion of the signatory's will towards commitment to the content of the document or record signed, without regard to the image, means, or form of the signature.

Accordingly, the electronic signature is every mark issued electronically from a person indicating their name or any of their characteristics, and expressing their consent to contract or dispose. This concept is valid for encompassing the various existing forms

¹. Official Gazette, No. 44, Year 42, op. cit., p. 24.

². Electronic signature: Data in electronic form attached to or logically associated with other electronic data used as a means of authentication

³. Same reference, p. 07

of the electronic signature, and even those that may appear in the future following the successive developments in the field of information and communication technology. It also achieves the conditions required in the signature in general through determining the identity of the signatory and indicating their consent to the content of the concluded disposition.

The essence of the difference between the electronic signature and the traditional signature lies in the medium or carrier upon which each is recorded. While the electronic signature relies on electronic media, the traditional signature relies on paper media terminated by a traditional signature.

Furthermore, while the traditional signature takes specific forms or images represented in the manuscript signature, the fingerprint, or the seal—with a variation among legislations regarding the recognition of all three forms or limiting it to one or two only—the legislations that addressed the electronic signature did not restrict it to a specific form or image. It can be letters, numbers, symbols, images, signs, or others; the important thing is that it allows for determining the identity of the signatory and distinguishing them from others.

In addition to the foregoing, it is possible through the electronic signature to deduce the content of the electronic document and secure it from modification by addition or deletion, by linking it to the electronic signature, such that any subsequent modification requires a new signature. Moreover, the electronic signature grants the document the character of an original document; thus, making it evidence pre-prepared for proof before any dispute arises between the parties to the transaction⁽¹⁾

Second: Forms of Electronic Signature

Based on the premise that the primary objective of the emergence of the electronic signature is to achieve confidence in electronic transactions, dealers in this field have attempted to exploit everything offered by advanced and renewable technologies in the field of information and communication technology to ensure that the electronic signature enjoys all the conditions required in the traditional signature, and consequently, the absolute equality between electronic records and traditional records in proof. This matter led to the existence of numerous forms of this type of signature depending on the technologies used therein, in a pursuit to make it more secure, and thereby gaining the trust of a greater number of dealers in the electronic field. Among the most important forms of electronic signature currently known, we mention by way of example: Signature via the card linked to the PIN code, the Biometric signature, and the Digital signature. Due to the importance of these three forms, we will address each of them in some detail as follows:

1- Signature via the Card Linked to the PIN Code: Signing by this method is done using a set of numbers or letters or both chosen by the owner of the signature to determine their personality, which no one else knows—unless they wish to communicate it to someone—and this method is called (N.I.P), which is an abbreviation for (*Numéros*

¹. See: Iman Mamoun Mohamed Suleiman: Conclusion and Proof of the Electronic Contract, op. cit., p. 253.

d'identification personnels)⁽¹⁾. This secret signature is often linked to plastic or magnetic cards, and other similar modern cards equipped with an electronic memory⁽²⁾. This type of electronic signature spreads particularly in the field of banking operations, i.e., electronic payment⁽³⁾.

2- Biometric Signature (*La signature Biométrique*): It is also called signature by personal properties because it relies on the distinct personal characteristics of individuals. According to this form of electronic signature, reliance is placed on one of the physical and behavioral characteristics of the human being, which are naturally assumed to differ from one person to another, such as: the personal fingerprint, the retina print, the voice print, the lip print, the properties of the human hand, the personal signature... A precise image of one of these physical characteristics of the person wishing to use the biometric signature is captured, then stored in an encrypted manner in the computer memory, and programmed in a way that makes it not issue its commands for dealing except after matching the dealer's print with the print stored in its memory, i.e., after verifying the identity and personality of the dealer⁽⁴⁾.

Falling under this image as well is the signature via the electronic pen, which entails that the person signs on the computer screen using a special pen. This requires computers with special specifications. The verification of the signature's validity is based on the movement of the electronic pen and the shapes it takes in terms of curves or twists, and other characteristics of the signatory's specific signature. An image of it is saved in the computer's memory to enable the comparison between the saved signature and the sent signature⁽⁵⁾.

This type of signature has been criticized on the grounds that the recipient can retain a copy of that signature and then re-apply it to any document drawn up on electronic media and attribute it to the owner of the signature. Nevertheless, this type of signature should not be absolutely rejected, as it can be beneficial in transactions conducted via Intranet and Extranet networks, as they are considered relatively secure networks. In addition, their users generally know one another⁽⁶⁾.

3- Digital Signature (*La signature Numérique*): This is the most widely used form of electronic signature. This type of electronic signature is executed by writing the signature and the document issued therein in the form of numbers, i.e., converting it into an unreadable and incomprehensible form, making it impossible for any other person or entity to understand or interpret this code. The intended recipient is the only one capable of deciphering this code using the key designated for that purpose. This means that the

1. It corresponds in English to the term (P.I.N), which is an abbreviation for (Personal Identification Number).

2. Among the cards currently used globally, we mention: Visa card, Mastercard, and American Express.

3. See: Ibrahim El-Desouki Abu El-Lail: Legal Aspects of Electronic Transactions: A Study of the Legal Aspects of Dealing via Modern Communication Devices "Electronic Mail", 1st Ed., Kuwait, Kuwait University, Scientific Publication Council, 2003, p. 158.

4. See: Iman Mamoun Ahmed Suleiman: Conclusion and Proof of the Electronic Contract, op. cit., p. 256, Ata Abdul Aati Al-Sanbati: Proof in Electronic Contracts: A Jurisprudential Study, paper submitted to the conference "Electronic Banking between Sharia and Law", op. cit., 1/471.

5. See: Ibrahim El-Desouki Abu El-Lail: Legal Aspects of Electronic Transactions, op. cit., pp. 258-259.

6. See: Iman Mamoun Ahmed Suleiman: Conclusion and Proof of the Electronic Contract, op. cit., p. 259.

digital signature process relies on two keys for encryption: one used to encrypt the digital signature by the signatory, which is the Private Key⁽¹⁾, and the second used to decrypt the code by the recipient, which is the Public Key⁽²⁾. This achieves securing the integrity of the electronic message on the one hand, and enables the verification of its validity and proving its attribution to the sender through its signing on the other hand⁽³⁾. The mechanism of working with these two keys will be clarified when we discuss encryption in a subsequent section.

Although these two keys are not identical, they are computationally linked. However, knowing the public key does not enable one to computationally reach the private key. This leads us to say that although many people may be aware of a signatory's public key and use it to verify their electronic signatures, they cannot discover that signatory's private key and use it to forge those signatures⁽⁴⁾. This makes the digital signature the most secure type of electronic signature because it achieves the highest degrees of confidence based on the fact that it⁽⁵⁾

- Using the digital signature realizes the link between the written document and the signature thereon.
- It guarantees the impossibility of interference in the content of the signature or the content of the document to which it is linked.
- It leads to the verification of the signatory's identity, and that the message signed by them is attributed to them, as they cannot deny the document attributed to them due to the existing link between the public and private keys.
- It achieves the confidentiality of the information contained in electronic documents, as they cannot be read except by the person to whom they were sent using the sender's public key.

For the digital signature to achieve this high degree of confidence and credibility, the presence of a neutral party is necessary. This party undertakes delivering the public key from the sender to the recipient, and issues electronic certificates determining the identity of the dealers and the validity of the information contained in their messages. This is known as "Certification and Authentication Authorities," which we will address in a separate section later.

Finally, we conclude that the mentioned forms of electronic signature differ in terms of the technologies used therein, and the degree of security and confidence achieved by each form. However, we cannot prefer one over the other, given that they are in

¹. The Algerian legislator defined the private key pursuant to the text of Article 2/8 of Law No. 15-04 defining the general rules related to electronic signature and electronic certification, which stated: "Private encryption key: is a string of numbers possessed exclusively by the signatory only, and used to create the electronic signature. This key is linked to a public encryption key." Official Gazette, No. 06, Year 52, op. cit., p. 07.

². As for the public key, the Algerian legislator defined it by stating: "Public encryption key: is a string of numbers made available to the public with the aim of enabling them to verify the electronic signature, and is included in the electronic certification certificate." Official Gazette, No. 06, Year 52, op. cit., p. 07.

³. See: Mohamed El-Morsi Zahra: Civil Protection for Electronic Commerce, op. cit., p. 236.

⁴. Safwan Hamza Ibrahim Issa: Legal Provisions for Electronic Commerce, PhD Thesis, Cairo University, Faculty of Law, Commercial Law Department, 2012, p. 178.

⁵. Iman Mamoun Ahmed Suleiman: Conclusion and Proof of the Electronic Contract, op. cit., pp. 169-170.

continuous development following the successive developments in the field of technologies employed therein. In addition, the search for achieving confidence and security in the electronic signature, and consequently the preservation of rights in the field of electronic transactions, makes the hypothesis of the appearance of new forms for it permanently existent. This justifies the reluctance of various legislatures to mention a specific form for the electronic signature, as all the definitions we mentioned, and those we did not mention, were formulated in a general manner without specifying a specific form or special method for its execution.

From here, it can be said that the only criterion for accepting a specific form or image for the electronic signature and recognizing it in proof is the extent to which the conditions required in the signature in general are met in this form.

Second: Guarantees of Confidence in the Electronic Signature

The guarantees of confidence in the electronic signature imply granting evidentiary validity to this type of signature. The evidentiary validity of the electronic signature in proof is determined through the extent to which it meets the conditions required in the ordinary (traditional) signature on the one hand, and through the technical guarantees capable of ensuring confidence in this type of signature, which will be clarified in the following:

1- Conditions of the Electronic Signature:

By referring to the legislations regulating the electronic signature, from which the latter derives its evidentiary validity, and which we mention by way of example and not limitation: European Directive No. 1999/93 related to electronic signatures, the UNCITRAL Model Law on Electronic Signatures of 2001, French Law No. 2000-230 of March 13, 2000, regarding the adaptation of evidence rules to information technologies related to the electronic signature, Executive Decree No. 2001-272 regarding the implementation of Article 1316-4 of the Civil Code related to the electronic signature, and Algerian Law No. 15-04 defining the general rules related to electronic signature and electronic certification... we find that they distinguished between two types of electronic signatures: The ordinary electronic signature, and the enhanced, secure, specified, or protected electronic signature. They made the enhanced electronic signature completely equivalent to the traditional or handwritten signature, provided it meets the following conditions: 1- That it is linked to the signatory alone. 2- That it allows for the identification of the signatory. 3- That it is created using means that enable the signatory to keep it under their exclusive control. 4- That it is linked to the data it authenticates in a manner that allows the detection of any alteration affecting it⁽¹⁾

¹. These conditions were included in: Article 2/2 of European Directive 1999/93/EC which stipulated: "2- 'advanced electronic signature' means an electronic signature which meets the following requirements: a) being uniquely linked to the signatory; b) capable of identifying the signatory; c) created using means that the signatory can maintain under their sole control; and d) linked to the data to which it relates in such a manner that any subsequent change of the data is detectable." OJ of the European Communities, 19.1.2000, L13, p14. And Article 1/2 of Decree No. 2001-272 of March 30, 2001, regarding the application of Article 1316-4 of the Civil Code related to the electronic signature, which stated: "'secure electronic signature': an electronic signature which, in addition, meets the following requirements: - be specific to the signatory; - be created by means that the signatory can maintain under their sole control; - guarantee with the act to which it is attached a link such that any subsequent modification of the

By looking at these conditions, we can point out that:

- Regarding the first and second conditions related to the electronic signature being linked to the signatory alone and allowing for the determination of its issuer's personality, they indicate that the electronic signature must provide definitive evidence of the signatory's person. This matter is self-evident even in the handwritten or traditional signature, whether done by manuscript, seal, or fingerprint, as determining the identity of the signatory who concluded a specific disposition is necessary in the field of proof. Accordingly, even if the electronic signature is in the form of numbers, letters, symbols, or sounds... it must ultimately enable the determination of its owner's identity and distinguishing them from others. This is realized in all forms of the electronic signature we referred to previously, as each relies on characteristics, properties, or codes distinguishing the person and determining their identity.
- Regarding the third condition, which requires that the electronic signature be created by means the signatory can keep under their exclusive control, the European Directive No. 1999/93/EC indicated in its Third Annex⁽¹⁾ some requirements capable of achieving security measures for the electronic signature. Its first paragraph obligated that these requirements ensure the following:
 - That the data used for generating the electronic signature can practically occur only once, and their confidentiality must be guaranteed.
 - That they enable obtaining sufficient confidence that the data used for generating the signature cannot be derived by inference, and that the signature is protected by the technical means available at the time of reliance.
 - That the data used for generating the electronic signature be protected in a reliable manner by the legitimate signatory against their use by others.

The second paragraph of the Annex indicated that the aforementioned requirements must not modify the data used for generating the electronic signature, nor prevent that data from being submitted to the signatory before the signature process.

The Algerian legislator adopted this Annex verbatim in the text of Article 11 of Law No. 15-04 defining the general rules related to electronic signature and electronic certification previously referred to⁽²⁾

The researcher believes that fulfilling these requirements is fundamentally linked to the level of development of the information systems technologies used. Consequently, it cannot be asserted that states are equal in achieving this matter due to the technological

act is detectable." OJ of the French Republic, 31 March 2001, p5070. These were also included in Article 07 of Algerian Law No. 15-04 defining the general rules organizing electronic signature and electronic certification, which stipulated: "The specified electronic signature is the electronic signature which meets the following requirements: 1- That it is created on the basis of a specified electronic certification certificate, 2- That it is linked to the signatory alone, 3- That it enables the identification of the signatory, 4- That it is designed by a secure mechanism specific to creating the electronic signature, 5- That it is created by means that are under the exclusive control of the signatory, 6- That it is linked to the data related to it, so that subsequent changes to this data can be detected." Official Gazette, No. 06, Year 52, op. cit., p. 08.

¹. OJ of the European Communities, 19.1.2000, L13, p20.

². Official Gazette, No. 06, Year 52, op. cit., p. 08

disparity among them. This means that every state must be keen to keep up with the successive developments in this field to achieve an acceptable degree of confidence in the electronic signature, and subsequently in electronic transactions as a whole.

- Regarding the fourth and final condition related to the signature being linked to the information it authenticates in a way that allows the detection of any attempt at modification in this information, this condition stems from the fact that protecting the electronic signature, and even the handwritten signature, is not an end in itself, as much as it is a protection for the signed document. Placing the signature on a document implies the direction of the signatory's will to commit to the legal effects resulting therefrom. Therefore, we say that for this condition to be realized, it is necessary to find an integration between the data contained in the document and the electronic signature, such that any modification or change in the data message or electronic document after its signing is detectable, and any modification or change in the signature contained in the electronic document leads to the modification of the entire document data, making it unfit for proof. This is what is understood from the texts of legislations regulating the electronic signature which provide that the authentication of the electronic signature necessarily leads to the authentication of the electronic document linked to it⁽¹⁾

In addition to these four conditions, we find that the Algerian legislator added, pursuant to the text of Article 7/1 of Law 15-04 mentioned above, another condition requiring that the specified electronic signature be created on the basis of a specified certification certificate. This was also referred to by the French legislator in Article 3/2 of Decree No. 272-2001 previously mentioned, as well as by most laws regulating the electronic signature, but not as a condition rather as a mechanism for authenticating the electronic signature and increasing its strength in evidence.

After clarifying the conditions required for the enhanced electronic signature, we must point out that the legislations regulating the electronic signature have arranged legal effects resulting from the distinction between the ordinary electronic signature and the enhanced electronic signature. These effects are that the latter alone enjoys the same legal value as the traditional or handwritten signature written on a paper medium. So that it is not understood by way of contradiction that the ordinary or simple electronic signature has no evidentiary validity, those same legislations indicated that it must not be stripped of its legal effectiveness or lose its value as evidence before the judiciary merely because it is not based on a certification certificate, or because it was not created via a secure mechanism⁽²⁾

¹. Ali Abu Mariya: The Electronic Signature and its Probative Force: A Comparative Study, Hebron University Journal for Research, Vol. 5, No. 2, 2010, p. 119.

². This is understood from the text of Articles 8 and 9 of Algerian Law No. 15-04 previously mentioned, which respectively stipulate: "The specified electronic signature alone is considered equivalent to the written signature, whether for a natural or legal person," "Without prejudice to the provisions of Article 8 above, the electronic signature cannot be stripped of its legal effectiveness or rejected as evidence before the judiciary due to: 1- Its electronic form, or, 2- It not relying on a specified electronic certification certificate, or, 3- It not being created via a secure mechanism for creating the electronic signature." (Official Gazette, No. 06, Year 52), op. cit., p. 08. This

This means that the evidentiary validity of the ordinary electronic signature in proof is subject to the discretionary power of the court or the judge, who may subject it to technical expertise to determine whether it is possible to consider it as having full evidentiary validity, or to consider it merely as a beginning of proof in writing⁽¹⁾. It also means that in the event an ordinary electronic signature and an enhanced electronic signature are presented to prove a specific disposition, the enhanced electronic signature takes precedence over the ordinary one, because the former is higher in evidentiary strength than the latter.

After this presentation of the two types of electronic signature, the conditions for the enhanced electronic signature, and the legal effects resulting from the distinction between them regarding evidentiary validity, we can say that the existence of the electronic signature in an electronic environment, the most important characteristic of which is instability and continuous successive development, makes it in need of technical guarantees that achieve legal recognition for it, regardless of whether it is simple (ordinary) or enhanced. This is what we will address in the following subsection.

2- Guarantees of Legal Recognition of the Electronic Signature:

Upon reviewing the legislations regulating the electronic signature, we find that they link the issue of equivalence between the electronic signature and the traditional or handwritten signature, and consequently the equivalence between electronic records and paper records, to the existence of technical guarantees that prevent the abuse of electronic technologies or their forgery. In other words, the strength of the electronic signature or document in evidence depends on the credibility of the information system used in its creation. We also find them emphasizing the necessity of the presence of a neutral third party that issues a certificate through which it authenticates the validity of the digital information issued by the person to whom the electronic signature is attributed⁽²⁾.

1- Technical Guarantees:

The problematic nature of the evidentiary validity of the electronic signature in proof is predominantly technical rather than legal, because the latter has become a settled matter after being organized by legislations at both the international and national levels. This means that the path capable of giving the electronic signature a validity or strength in evidence comparable to that granted to the traditional or handwritten signature, i.e., achieving equivalence between the two signatures, lies in establishing a reliable technical system that ensures the credibility of the information issued through it, along with the elements and complementary programs that enhance this credibility for this system.

corresponds to the text of Article 5/1 and 2 of European Directive No. 1999/93/EC, and the text of Article 6/3 of the Model Law on Electronic Signatures issued by the United Nations Commission on International Trade Law 2001.

¹. See: Mohamed Lawrence Obeidat: Proof of the Electronic Document, 1st Ed., Amman, Dar Al-Thaqafa for Publishing and Distribution, 2005, pp. 159-160.

². See: Basil Youssef: "Legal Recognition of Electronic Documents and Signatures in Comparative Legislations", Journal of Legal Studies, Legal Studies Department at Bayt al-Hikma, Baghdad, No. 02, Vol. 03, (1422H-2001), p. 21.

By referring to studies that have addressed the technical systems used in the field of the electronic signature, we find them focusing on the fact that the information system capable of achieving the desired credibility in this field must be⁽¹⁾

- A system enjoying the necessary guarantees for its good performance, so as to persuade judges to grant greater trust to electronic documents.
- A system guaranteeing a methodical and organized preservation and protection of all occurring information operations.
- A system capable of ensuring that the storage media where the information data is registered record the number of times this data is inspected, so as to control the technical possibility of copying digital data that remains present even if it is registered inside an optical disc.
- A system allowing for precise determination of the date of sending and receiving electronic documents and ensuring that they were received by the person to whom they were sent, without modification or prejudice to their integrity.

Despite the importance of these guarantees, even if they are present in a specific system, it is not possible to assert its ability to achieve a complete degree of security (100%) where the possibility of error and hacking is non-existent.

Perhaps the most important technical guarantees available until now are encryption technologies, which rank at the forefront of the innovative means in the field of achieving the security and integrity of contracts and documents concluded and exchanged via the Internet. We will try to shed light on this technology, even briefly, to clarify the extent of its ability to achieve credibility for the electronic signature, especially since we showed when addressing the forms of the electronic signature that the digital signature—which relies on this technology as its basis—is considered the most recent of these forms and the most widely used, as follows:

A- Definition of Encryption (Cryptography): Encryption is the process of converting information into codes that are incomprehensible to the public, so that unauthorized persons cannot access or understand the information⁽²⁾. Many legislatures have defined it, including for example:

- French Legislation: Pursuant to Article 28 of Law No. 90-1170 regarding the regulation of telecommunications, which defined encryption means and tools as: "All techniques aiming, through secret conventions, to transform readable information or signals into information or signals unintelligible to third parties, or to perform the reverse operation, using hardware or software designed for this purpose"⁽³⁾
- Tunisian Legislation: The law on electronic exchanges and commerce⁽⁴⁾ defined it pursuant to Article 2/5, which stated: "Encryption: either the use of non-circulated

¹. Basil Youssef: Legal Recognition of Electronic Documents and Signatures, op. cit., pp. 22-23.

². Elias Nassif: International Contracts: The Electronic Contract in Comparative Law, op. cit., p. 243.

³. On entend par prestation de cryptographie toute les prestations visant à transformer à l'aide de conventions secrets des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens matériels, ou logiciels conçus à cet effet

⁴. Law No. 83 of 2000 dated August 9, 2000, relating to electronic exchanges and commerce, op. cit

codes or signals whereby the information intended to be passed or sent becomes unintelligible to third parties, or the use of codes or signals without which the information cannot be accessed."

From the foregoing, we conclude that encryption is the use of specific means or methods that allow hiding the content of information by converting it into an unreadable form with the aim of protecting it from any modification or unlawful use⁽¹⁾. This is done through a secret key used by the sender, and the message is restored to its original form in the same way, i.e., by using a secret key possessed by the person to whom this message is addressed.

Technically, encryption means rewriting the data message before sending it using a specific key that assumes a link between data and numbers, provided that the recipient has the ability to retrieve the message in its original form before encryption⁽²⁾. This is done either by using the same key used by the sender, or by using another key depending on the type of encryption used, as we will clarify in the following subsection.

B- Types of Encryption: The types of encryption relate primarily to the key used for encryption and for decryption. This key may be a single key used by both the sender and the recipient, known as symmetric encryption, or there may be two keys, one possessed by the sender and the other by the recipient, known as asymmetric encryption. We will attempt to explain each as follows:

1^o- Symmetric Encryption: This type of encryption relies on using a single key to encrypt the message on the one hand, and to decrypt the code on the other. This means that the same key is in the possession of both the sender and the recipient. It is assumed that no one else knows it, and that they must maintain its confidentiality throughout the period of its use.⁽³⁾

This system is criticized for relying on a single key that must be sent secretly and securely to the recipient so they can restore the message to its original form. This sending process cannot be guaranteed to be 100% secure, as it usually takes place via the internet, giving the possibility of it being hacked by third parties and the key being accessed. It is also criticized on the grounds that this system assumes prior knowledge between the sender and the recipient, which may not be realized in electronic commerce, which often takes place between two distant persons who do not know each other. These criticisms led to a decline in the use of this type of encryption⁽⁴⁾

2^o- Asymmetric Encryption: The failure of the symmetric encryption system to achieve the purpose of encryption—namely, protecting the business and data exchanged via modern communication means in general and the internet in particular—was a reason

¹. Abd al-Fattah Bayoumi Hijazi: The Electronic Signature in Comparative Legal Systems, 1st Ed., Alexandria, Dar Al-Fikr Al-Jami'i, 2005, p. 31.

². Raafat Radwan: The World of Electronic Commerce, op. cit., p. 80.

³. See: Ali Sayed Qassem: "Some Legal Aspects of the Electronic Signature", Journal of Law and Economics for Legal and Economic Research, Faculty of Law, Cairo University, No. 72, 2002, p. 13.

⁴. See: Mohamed Fawzi Al-Mutalaqah: The Concise in Electronic Commerce Contracts, op. cit., pp. 163-164, Raafat Radwan: The World of Electronic Commerce, op. cit., p. 85, Basil Youssef: Legal Recognition of Electronic Documents and Signatures in Comparative Legislations, op. cit., p. 25, Ali Sayed Qassem: "Some Legal Aspects of the Electronic Signature", op. cit., p. 13.

for searching for an alternative to achieve this purpose. Consequently, technicians arrived at another encryption system: asymmetric encryption.

This system relies on using two types of keys instead of one type in the previous system. The first key is called the public key (*clé publique*), and the second key is the private key (*clé privée*). A strong mathematical relationship links these two keys, without implying that one can be deduced from knowing the other, as we pointed out when discussing the digital signature.

The mechanism of this type of encryption is that the private key is known to only one party or one person, who is the sender, while the public key is known to more than one person or entity. The public key can decrypt the code of the message that was encrypted by the private key, and it can also be used to encrypt messages sent to the owner of the private key, without it being possible to use the public key to decrypt a message encrypted by it. This means that the owner of the private key is the only one capable of decrypting messages encrypted with the public key⁽¹⁾.

We can clarify the encryption mechanism through a model showing the use of two persons (Alice) and (Bob) of asymmetric encryption to encrypt the transactions concluded between them.

Among the common programs in this type of encryption is the (PGP) program, which is an abbreviation for (Pretty Good Privacy), designed by the American "Phil Zimmerman" in 1991. It is a program distinguished by a high degree of security and precision, to the extent that some consider it a program that is almost impossible to crack⁽²⁾.

Due to the efficacy of asymmetric encryption in achieving protection for data exchanged via the internet in particular, it has been used in the electronic signature. Thus, the digital electronic signature appeared, which we saw is based on two keys—public and private—meaning it relies on asymmetric encryption technology. This is perhaps what made it the most widely used type of electronic signature, as we previously mentioned.

However, what should be noted here is that despite the existence of technical guarantees with a high degree of confidence and security capable of achieving credibility for the electronic signature, and consequently for the electronic document on which this signature exists—and the most important of which was asymmetric encryption, whose mechanism of operation we clarified and for which we gave an applied model, and about which it was said that the possibility of cracking it is almost impossible—this does not mean that this type of encryption is free from difficulties. Practical reality has shown that there are many problems facing it, which are essentially represented in: What guarantees that the public key actually belongs to the user in possession of the private key? In addition to the difficulties related to verifying the capacity of the signatory, their will, and the absence of fraud in the transaction....

¹. See: Fawzi Al-Mutalaqah: The Concise in Electronic Commerce Contracts, op. cit., p. 165.] [8: -() Kolb Romain: Signature électronique, GALLIS Ingenierie, 31/10/2008, p. 4-5, Study published on the site: <http://www.calais-conseil.com> 03/04/2015 at 11h 38m.

². Basil Youssef: Legal Recognition of Electronic Documents and Signatures in Comparative Legislations, op. cit., p. 25.

Legislations regulating the electronic signature attempted to find a solution to these practical problems by finding a neutral third party that authenticates the identity of the possessors of the keys used in the encryption process, the integrity of the transaction, and the availability of consent. It even undertakes the delivery of encryption keys, and this is done by issuing an electronic certificate used when necessary.

Secondly: Electronic Authentication

The endeavor of legislations regulating electronic transactions and commerce on the one hand, and regulating electronic signatures on the other, to achieve equivalence and consequently equality between electronic records and signatures and traditional records and signatures, made them approve a set of procedures and means capable of assisting in achieving this goal. Among these procedures was "Electronic Authentication," which "is considered a secure technical means for verifying the validity of the signature or document, where it is attributed to a specific person or entity through a trusted party or neutral third party called the certification service provider or authentication services provider"⁽¹⁾

1- Electronic Authentication Authorities:

Electronic authentication authorities are the competent bodies for issuing electronic authentication certificates capable of achieving confidence and security in electronic transactions. Because these transactions, as we have indicated since the beginning of this thesis, are characterized by a special nature, given that they take place between distant parties who do not know each other, and may not even have the possibility of meeting at any stage of concluding the transaction, it is necessary to provide a set of guarantees that help determine the identity of these dealers, their capacity, the validity of their will, in addition to ensuring the nature and content of the transaction.

Electronic authentication authorities, therefore, existed to achieve these guarantees. Therefore, they were defined as: "Public or private bodies or entities that issue electronic certificates whose function is to identify the person holding them and their capacity, and authenticate their electronic signature and the deals they conduct via the internet"⁽²⁾, or they are: "A neutral, independent, public or private body or organization that acts as an intermediary between dealers to document their electronic transactions by issuing electronic certificates"⁽³⁾

The European Directive No. 1999/93/EC regarding the common framework for electronic signatures defined them in Article 2/11 as: "An entity or natural or legal person who provides certificates or offers other services related to electronic signatures"⁽⁴⁾. The UNCITRAL Model Law on Electronic Signatures issued by the United Nations

¹. Mohamed Hussein Mansour: Traditional and Electronic Proof, 1st Ed., Alexandria, Dar Al-Fikr Al-Jami'i, 2006, p. 289.

². See: Basil Youssef: Legal Recognition of Electronic Documents and Signatures in Comparative Legislations, op. cit., p. 26.

³. See: Said El-Sayed Kandil: The Electronic Signature: Its Nature, Forms, and Evidentiary Validity between Internationalization and Borrowing, 1st Ed., Alexandria, Dar Al-Jami'a Al-Jadida for Publishing, 2004, pp. 75-76, Iman Mamoun Ahmed Suleiman: Conclusion and Proof of the Electronic Contract, op. cit., p. 309.

⁴. prestataire de service de certification: toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques;". OJ of the European Communities, 19.1.2000, L13, p14.

Commission on International Trade Law in 2001 defined them in Article 2(e) which stated: "'Certification service provider' means a person who issues certificates and may provide other services related to electronic signatures;"⁽¹⁾

As for the Algerian legislator, we find that they defined certification authorities pursuant to Article 2⁽²⁾ of Law 15-04 defining the general rules related to electronic signature and electronic certification. However, they differentiated between the "Trusted Third Party", which they defined in paragraph 11 of this Article as: "A legal person who grants specified electronic certification certificates, and may provide other services related to electronic certification for the benefit of interveners in the government sector," and the "Electronic Certification Service Provider," who they defined in paragraph 12 of the same Article as: "A natural or legal person who grants specified electronic certification certificates, and may provide other services in the field of electronic certification." Thus, they specialized the Trusted Third Party in services related to electronic certification for the benefit of interveners in the government sector, whom they defined pursuant to paragraph 13 of the same Article 02 as: "Public institutions, administrations, and bodies specified in the applicable legislation, national institutions, and interveners in inter-bank exchanges, as well as any person or entity belonging to the government sector by virtue of its nature or missions." Other than this category, they are subject to the authority of the electronic certification service provider.

It is observed regarding these definitions that they agree that certification bodies or authorities are independent, neutral bodies that may be natural or legal persons. They may also be public bodies established by state intervention or private bodies that document electronic transactions upon the request of their parties.

The tasks that certification authorities can perform can be summarized as follows⁽³⁾

1. Verifying the identity of the signatory: This constitutes a primary obligation for these authorities. They issue an electronic authentication certificate through which they authenticate the electronic signature, meaning they testify to the validity of the signature and its attribution to the person who issued it. This primary obligation entails determining the legal capacity to deal and contract for the parties to the electronic transaction, in addition to verifying the content of this transaction, its integrity, and its freedom from fraud and deceit, such as tracking commercial websites on the internet to investigate their seriousness and credibility. If it is proven to them that one of those sites is insecure, they warn dealers with that site by sending messages clarifying the lack of credibility of that site.
2. Issuing the digital signature: And the authentication certificate for this signature, by which they testify to the validity of the signature and its attribution to its issuer.

¹. United Nations: UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, United Nations Publications, New York 2002, Sales No. A.02.V8, p. 02.

². United Nations: UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, United Nations Publications, New York 2002, Sales No. A.02.V8, p. 02.

³. See: Ibrahim El-Desouki Abu El-Lail: Legal Aspects of Electronic Transactions, op. cit., pp. 177-182, Abd al-Fattah Bayoumi Hijazi: The Electronic Signature in Comparative Legal Systems, op. cit., p. 134, Iman Mamoun Ahmed Suleiman: Conclusion and Proof of the Electronic Contract, op. cit., p. 314.

They also undertake the issuance of keys related to encryption, whether private keys or public keys. Consequently, these authorities guarantee the link between a private key and a public key. They also transfer the private key and its electronic signature in a reliable manner without retaining a copy of the signature and its private key.

3. Maintaining electronic registers: Specialized in electronic signatures, in which they clarify which are valid, which have been cancelled or invalidated, and which have been suspended.

In order for certification authorities to perform the above-mentioned tasks, they must respond to a set of conditions, including those stated in the Algerian Law No. 15-04 defining the general rules related to electronic signature and electronic certification. Article 33 of this Law stated: "The activity of providing electronic certification services is subject to a license granted by the Economic Authority for Electronic Certification." Article 34 of the same Law stated: "Every applicant for a license to provide electronic certification service must meet the following conditions: - To be subject to Algerian law in the case of a legal person or hold Algerian nationality in the case of a natural person, - To enjoy sufficient financial capacity, - To possess proven qualifications and experience in the field of information and communication technologies for the natural person or the manager of the legal person, - To not have been previously convicted of a felony or misdemeanor incompatible with the activity of providing electronic certification services."

Through these two texts, we observe that the Algerian legislator stipulated the following in the service provider:

1. Obtaining a license from the Economic Authority for Electronic Certification: The same Law indicated that this authority is appointed by the authority in charge of regulating post and electronic communications (Article 29), and defined its tasks pursuant to Article 30. These are numerous tasks, including: granting licenses to electronic certification service providers after the approval of the authority, and taking the necessary measures to ensure the continuity of services in the event of the electronic certification service provider's inability to provide its services.

Accordingly, it can be said that the Algerian legislator acted correctly by making certification authorities subject to state supervision, as the requirement of a license imposes a kind of trust and security on the work of these authorities. It leads to verifying the availability of conditions that make the certification authority worthy of practicing this work, thereby reducing the chances of fraud in the work of these authorities. The legislator also acted correctly by making it among the tasks of the Economic Authority for Electronic Certification to take the necessary measures to ensure the continuity of services in the event of the electronic certification service provider's inability to provide its services. This reduces the chances of the interests of dealers—dependent on the issuance of certificates by certification authorities—being exposed to frequent disruption. This is of great importance in the commercial field, and especially in electronic

commercial transactions, as they are fundamentally characterized by speed and the inability to exceed automatically set deadlines.

2. Subjection to Algerian law in the case of a legal person and enjoyment of Algerian nationality in the case of a natural person: This means that the Algerian legislator does not license non-Algerians, nor legal persons subject to foreign law, to provide electronic certification services on Algerian territory.
3. Enjoying sufficient financial capacity: This means that the financial position of the natural or legal person wishing to provide electronic certification services has a consideration in Algerian legislation. The reason that prompted the Algerian legislator to take the financial aspect into account is likely that electronic certification services rely on precise technological techniques. Moreover, these techniques are in continuous and rapid development, and the certification authority must keep up with these developments to ensure the performance of its services with a high degree of efficiency. This matter is very costly, especially since we are among the countries importing technology, not among those producing it.

4- That the natural person or the manager of the legal person wishing to provide electronic certification service enjoys proven qualifications and experience in the field of information and communication technologies: This condition is considered among the conditions related to the professional competence of certification authorities. The Algerian legislator stipulated proven experience in this field, meaning that whoever submits an application to be granted a license to provide these services must submit proof of the necessary experience qualifying them to perform this task, especially since it relies on advanced techniques in the field of information and communication technologies, which requires knowledge and specialization. The legislator is correct in stipulating such a condition because they must ensure high efficiency in performing these tasks to gain the trust of dealers in the commercial field and encourage them to engage in electronic transactions.

5- That the applicant for the license has not been previously convicted of a felony or misdemeanor incompatible with the activity of providing electronic certification services: Meaning that they must not have committed a crime of forgery or electronic fraud, for example. This condition is a precaution on the part of the legislator regarding the data and personal information of dealers in this field, who are required to place their full trust in the certification authority and provide it with all the private information required by the service it performs for them.

In addition to these conditions, it is incumbent upon certification authorities to maintain the confidentiality of information and the secrets of the private lives of dealers with them⁽¹⁾. Any breach of one of the obligations incumbent upon them exposes them to liability⁽²⁾

¹. The Algerian legislator stipulated in Article 42 of the aforementioned Law that: "The electronic certification service provider must preserve the confidentiality of data and information related to the granted electronic certification certificates."

². This was included in Articles 53 and 54 of the aforementioned Law. See: Official Gazette, No. 06, Year 52, op. cit., p. 13.

2- Electronic Certification Certificates:

Electronic authentication certificates are the certificates issued by certification authorities, licensed by the responsible authorities in the state, to certify that the electronic signature is a valid signature attributed to its issuer, and meets the required conditions and controls as reliable proof of evidence⁽¹⁾.

The UNCITRAL Model Law on Electronic Signatures of 2001 defined them in Article 2/b as: "A data message or other record that confirms the link between the signatory and signature creation data"⁽²⁾.

As for European Directive No. 1999/93/EC regarding the common framework for electronic signatures, it distinguished between two types of electronic certificates issued by electronic certification authorities: A simple electronic certificate linked to data and information related to the verification of the signature of a specific person and confirming the identity of that person⁽³⁾, and a qualified electronic certificate, which is the certificate that meets the requirements listed in Annex I of this Directive and is provided by a certification service provider that meets the requirements listed in Annex II⁽⁴⁾. This is what the Algerian legislator also adopted, who defined the electronic certification certificate pursuant to Article 2/7 of Law 15-04 as: "A document in electronic form that proves the link between the electronic signature verification data and the signatory." Then they referred to the specified electronic certification certificate pursuant to Article 15 of the same Law, meaning that the Algerian legislator distinguishes between two types of electronic certification certificates, just like the European Directive.

From these definitions, we deduce that the objective of issuing electronic certification certificates is to confirm the attribution of the electronic signature, and consequently the electronic document, to the person from whom it was issued, and that their signature is a valid signature. These certificates also confirm that the data signed by the signatory is correct and free from any tampering or change, meaning it becomes authenticated data that cannot be denied, verified through secure technical systems and information systems that make the submitted certificate a means to enhance confidence among dealers⁽⁵⁾.

For the electronic certification certificates to achieve the purpose of their issuance, they must contain specific data determined by the Algerian legislator pursuant to Article 15/3 of Law 15-04, which stated: "The (specified electronic certification certificate) must contain in particular: A- An indication that this certificate was granted as a specified electronic certification certificate; B- Identification of the Trusted Third Party or the licensed electronic certification service provider issuing the electronic certification certificate, as well as the country in which they reside; C- The name of the signatory or

¹. Ibrahim El-Desouki Abu El-Lail: Legal Aspects of Electronic Transactions, op. cit., p. 183.

². United Nations: UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, op. cit., p. 02.

³. Article 1/9: "certificat: une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne.

⁴. Article 1/10: "certificat qualifié, un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II

⁵. Ibrahim El-Desouki Abu El-Lail: Legal Aspects of Electronic Transactions, op. cit., p. 183.

the pseudonym that allows their identification; D- The possibility of including a specific capacity for the signatory when necessary, according to the purpose of using the electronic certification certificate; E- Data related to the verification of the electronic signature, which is consistent with the electronic signature creation data; F- The indication of the start and end of the validity period of the electronic certification certificate; G- The identification code of the electronic certification certificate; H- The specified electronic signature of the electronic certification service provider or the Trusted Third Party granting the electronic certification certificate; I- The limits of use of the electronic certification certificate when necessary; J- The limits of the value of transactions for which the electronic certification certificate may be used, when necessary; K- The indication of the document proving the representation of another natural or legal person, when necessary."

Conclusion

The data contained in an electronic certification certificate constitute essential elements for its legal validity under Algerian law. In this regard, the trusted third party, or the electronic certification service provider, bears legal responsibility for any damages that may arise from the inaccuracy of such data, any breach relating thereto, or the failure to revoke the certificate when revocation becomes legally required.

However, due to the absence of implementing regulations clarifying the definitive form and structure of electronic certification certificates, and considering that the practical application of such certificates has not yet been fully operational in Algeria, this study has relied on presenting a model of a certification certificate issued by the National Agency for Electronic Certification of the Republic of Tunisia.

Furthermore, the Algerian legislator grants the trusted third party or the electronic certification service provider the authority to impose certain restrictions on the use of the electronic certification certificates it issues. Such restrictions may include indicating the limitations on the use of the certificate or specifying the maximum value of transactions in which the certificate may be utilized. Nevertheless, these restrictions must be clearly understandable to third parties. Similar provisions are also reflected in the European Directive on the legal framework for electronic signatures, particularly in Article 6(3–4).

In conclusion, the present research paper highlights several key findings:

First, in response to the evolving requirements of electronic commerce—characterized by the absence of paper-based documentation and the increasing reliance on electronic records instead of traditional paper documents—it has become necessary to adopt a new form of signature known as the electronic signature. This form of signature has gained widespread international recognition. The United Nations, through the United Nations Commission on International Trade Law (UNCITRAL), adopted the Model Law on Electronic Signatures. Subsequently, many countries enacted national legislation to regulate and legally recognize electronic signatures. Algeria has followed this global trend by enacting the Law on Electronic Signature and Electronic Certification. Although this legislation was adopted relatively late, it nevertheless represents an important step by the Algerian legislator in adapting to technological developments in this field.

Second, many countries have sought to enhance trust in electronic signatures by ensuring the highest possible level of security through advanced encryption technologies. In addition, neutral certification authorities have been established to issue authentication certificates that strengthen the credibility of electronic signatures and facilitate their use. Consequently, this contributes to increasing the confidence of users and economic actors in electronic documents, which are gradually replacing traditional paper-based documents in commercial transactions.

References

Arabic References

- Anwar Sultan, *Rules of Evidence in Civil and Commercial Matters: A Study in Egyptian and Lebanese Law*, Beirut: University Printing and Publishing House, 1984.
- Najwa Abu Haiba, *Electronic Signature: Definition and its Evidentiary Value*, Cairo: Dar Al-Nahda Al-Arabia, n.d.
- Mohamed Al-Morsi Zahra, *Civil Protection of Electronic Commerce*, 3rd ed., Cairo: Dar Al-Nahda Al-Arabia, n.d.
- Iman Maamoun Ahmed Suleiman, *Formation and Proof of the Electronic Contract: Legal Aspects of E-Commerce Contracts*, Alexandria: New University Publishing House, 2008.
- Ali Sayed Qassem, "Some Legal Aspects of the Electronic Signature," *Journal of Law and Economics for Legal and Economic Research*, Issue 72, 2002.
- Ibrahim Al-Dessouki Abu Al-Lail, *Legal Aspects of Electronic Transactions: A Study of Legal Issues in Communication through Modern Means (Electronic Correspondence)*, 1st ed., Kuwait: Kuwait University, Scientific Publishing Council, 2003.
- Safwan Hamza Ibrahim Issa, *Legal Provisions of Electronic Commerce*, PhD Dissertation, Faculty of Law, Cairo University, 2012.
- Ali Abu Mariya, "Electronic Signature and its Evidentiary Value: A Comparative Study," *Hebron University Research Journal*, Vol. 5, Issue 2, 2010.
- Mohamed Lawrence Obeidat, *Proof of the Electronic Document*, Amman: Dar Al-Thaqafa for Publishing and Distribution, 2005.
- Basil Youssef, "Legal Recognition of Electronic Documents and Signatures in Comparative Legislation," *Legal Studies Journal*, Department of Legal Studies, Bayt Al-Hikma, Baghdad, Issue 2, Year 3, 2001.
- Abdel Fattah Bayoumi Hegazy, *Electronic Signature in Comparative Legal Systems*, 1st ed., Alexandria: Dar Al-Fikr Al-Jamii, 2005.
- Mohamed Hussein Mansour, *Traditional and Electronic Evidence*, 1st ed., Alexandria: Dar Al-Fikr Al-Jamii, 2006.
- Said Al-Sayed Qandil, *Electronic Signature: Its Nature, Forms and Evidentiary Value between Internationalization and Adaptation*, 1st ed., Alexandria: New University Publishing House, 2004.

Legal Texts and International Instruments

- United Nations Commission on International Trade Law (UNCITRAL), *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment*, United Nations Publications, New York, 2002.
- United Nations General Assembly Resolution No. 56/80 adopting the *UNCITRAL Model Law on Electronic Signatures*, 24 January 2002.
- Law No. 15-04 of 1 February 2015 establishing the general rules relating to electronic signature and electronic certification, Official Journal of the People's Democratic Republic of Algeria, No. 06, 10 February 2015.
- European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.
- Decree No. 2001-272 of 30 March 2001 implementing Article 1316-4 of the French Civil Code relating to electronic signatures.

Foreign References

- Paule Robert, *Le Nouveau Petit Robert de la Langue Française*, revised under the direction of Josette Rey-Debove and Alain Rey, Paris: Sejer Editions, 2008.
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities, 19 January 2000.
- *Journal Officiel de la République Française*, 14 March 2000.
- *Journal Officiel des Communautés Européennes*, 19 January 2000.
- *Journal Officiel de la République Française*, 31 March 2001.
- Kolb Romain, *Electronic Signature*, Gallis Ingénierie, Study published on the website: <http://www.calais-conseil.com> (consulted 03 April 2015).